Airport Vulnerability Assessment – An Analytical Approach

NDIA Security Technology Symposium
Williamsburg, VA, June 15-18, 1998

Author: Rick Lazarick, FAA Technical Center, Aviation Security R&D

ABSTRACT

The Airport Vulnerability Assessment Project (AVAP), which is currently in progress, is the direct result of congressional funding of recommendation 3.13 of the White House Commission on Aviation Safety and Security. This project takes a new approach to the assessment of US commercial airports. AVAP uses automation, analytical methods and tools to evaluate vulnerability and risk, and to analyze cost/benefits in a more quantitative manner.

This paper addresses both the Process used to conduct this program as well as an unclassified look at the Results which have been achieved for the initial airport assessments.

The Process description covers the acquisition approach, the project structure, and a review of the various methodologies and tools being used by the 8 individual performing organizations (Battelle, BDM, SAIC, Lockwood Greene, CTI, Abacus Technology, Science and Engineering Associates, and the Naval Facilities Engineering Service Center). The tools described include ASSESS, SAM, RiskWatch, CASRAP and BlastFX. Included in the process is the establishment and use of an advisory panel made up predominantly of experts from the National Laboratories (Sandia, Oak Ridge, Argonne and Brookhaven).

The Results portion addresses the findings and products resulting from the initial airport assessments. High level (unrestricted) summaries of the results are presented, along with initial trends in commonly recommended security improvements (countermeasures). Emphasis is placed on positive noteworthy findings, showcasing the approach taken by airports with particularly good security practices. A summary of significant Lessons Learned is provided.

To conclude this paper, a project status and anticipated schedule for the next year is presented.

Introduction

The Federal Aviation Administration (FAA) sponsored Airport Vulnerability Assessment Project is the direct result of Congressional funding of recommendation 3.13 of the White House Commission on Aviation Safety and Security. Initiated in April 1997, this project is now just over one year old and significant progress has been achieved. This paper addresses the first round of airport assessments that will be completed in FY 98. What makes this project significantly different from all of the previous airport assessments is that it takes a new approach to the assessment of US commercial airports, using automated, analytical methods and tools to evaluate vulnerability, risk and cost/benefits in a more quantitative manner.

The following sections of this paper will trace the progression of the project from its inception to its current status. First is a description of the procurement process used to expedite the contracting of these vulnerability assessments and a summary of the technical approaches being employed. Next is a discussion of some generalized results of the assessments that have been completed. Finally, the plans for continuing this project are provided.

The Airport Vulnerability Assessment Process

To establish the project requirements and to assure that the assessments are conducted with a common threat definition, the FAA developed a detailed statement of work (sow) which established the minimum requirements for all performing organizations in terms of tasks and deliverables. Additionally, a set of 16 unique threat scenarios were established by the FAA. These generic threat scenarios defined the target (e.g. passenger aircraft), the threatening act (e.g. bombing), the aggressor (e.g. terrorist) with characteristics (e.g. originating passenger, non-suicidal), and the contraband (e.g. improvised explosive device, in luggage). These generic threat scenarios were then used by the contractors at each airport, and modified as required to fit the characteristics of that site. The FAA solicited all Category X and I airports looking for volunteer airports to participate in this effort. In all, 29 airports offered to participate.

One of the distinguishing characteristics of this AVAP is the acquisition strategy employed. The FAA, taking advantage of the acquisition reform policies recently afforded to the agency, used a combination of directed procurements and competitive awards to achieve contract arrangements with 8 different performing organizations in a period of only five months. In addition, the statement of work included a novel approach, in that a minimum requirement was established for airport vulnerability assessment. However, the contractors were encouraged to add to this minimum, any aspects of airport assessment which they felt would satisfy the needs of the airport security planners, such as risk assessment, cost-benefit analysis and cost-effectiveness of proposed countermeasures. Since the contracts were to be let as fixed priced contracts, the degree of additional analysis effort (beyond the minimum requirements of the SOW) was described in the technical proposals, and price was not used as critical evaluation criteria.

The objective was to obtain a wide range of vulnerability assessment approaches, utilizing several different quantitative methods and various automated tools. The clearly stated theme of this acquisition was “Do It Your Way”, meaning that the FAA spells out the fundamental aspects of the effort (What needs to be done), and the contractor is completely free to establish the methodology for the assessment (How it will be done). This approach, as you will see, resulted in a wide range of methods and tools.

Six airports were assigned to three performers based upon the FAA’s knowledge of their vulnerability assessment experience via a non-competitive directed procurement and a Military Interdepartmental Purchase Request (MIPR). (see table of performing organizations and assigned airports).

The competitive procurement process was used to contract five additional performing organizations. Initially, a Screening Information Request (SIR) was issued, and twelve organizations responded with corporate capability and experience statements. Upon FAA review, six of these were selected to receive the request for proposal (RFP), and a bidders conference was conducted. Formal technical and price proposals were submitted, and upon review by the FAA, five of the bids were awarded contracts for 1 or 2 airport assessments. From SIR announcement to contract award, this streamlined acquisition process took a mere 15 weeks.

ORGANIZATION	ASSIGNED AIRPORT
Abacus Technology Inc.	Denver (DEN)
	Detroit (DTW)
Battelle	Cincinnati (CVG)
	Louisville (SDF)
	Salt Lake City (SLC)
BDM Federal	Atlanta (ATL)
	Boston (BOS)
Counter Technology Inc.	San Juan (SJU)
Lockwood Greene Technology	Colorado Springs (COS)
Naval Facilities Engineering Service Center	Seattle-Tacoma (SEA)
	San Francisco (SFO)
SAIC	Miami (MIA)
	Jacksonville (JAX)
Science & Engineering Associates	Orlando (MCO)
	Newark (EWR)

Methodologies

The intent of the acquisition process was to obtain contractor services which represented a wide range of technical approaches to airport vulnerability assessment. As a group, the contractors’ approaches do represent a highly diverse set of assessment techniques, each of them proven in previous facility vulnerability assessment efforts primarily for the DOE, DOD and some public access facilities. The challenge now is to evaluate how well each of these techniques can be applied to US domestic airports. The following paragraphs briefly outline the basic approach and any automated tools being used by each of the contractors in this assessment.

Abacus Technology Inc.

The Abacus Team approach uses a combination of quantitative and qualitative analyses. The quantitative approach is supported by the use of the Security Assessment Model (SAM) originally developed for the NFESC. It is a detailed facility assessment tool with emphasis on detection opportunities, delay timing, response force timing and interdiction success. This tool strictly assesses facility vulnerability. In addition, Abacus is using the commercial product RiskWatch to assess the overall airport facility. RiskWatch includes vulnerability assessment, identification of potential countermeasures, risk analysis and cost-benefit analysis. Limited testing is included in the Abacus approach.

Battelle

The Battelle Team uses two complimentary techniques in their analysis. First is a manual technique known as the Analytical Risk Management (ARM) process originally developed by the CIA. ARM is a threat, vulnerability and risk assessment process that relies heavily on the expert opinions of the assessment team members. Additionally, the Civil Aviation Security Risk Analysis Process (CASRAP) developed by Akela for the FAA was used to assess the airport as a whole, and to validate the ARM methodology. CASRAP is based on an earlier product, SASSY, with a specific focus on US airport characteristics. It also includes vulnerability, risk and cost-benefit analyses. Very little testing is included in the Battelle approach.

BDM Federal

The BDM team includes RiskWatch, Inc., the developers of the tool "RiskWatch", which is the primary focus of their assessment method. RiskWatch addresses the analysis of vulnerability, risk and cost-benefits for the candidate countermeasures. RiskWatch is a commercial product, which was previously adapted to be specific to US airports. For scenarios involving the analysis of explosive blast effects, BDM uses the BlastFX model, which they developed under contract to the FAA. The model estimated building structural damage as well as the extent of human injury. The BDM approach does not depend upon testing, but does involve extensive questionnaires for the airport and air carrier employees to complete.

Counter Technology Inc. (CTI)

CTI uses both a quantitative and a qualitative approach to airport assessment. The quantitative approach uses a scenario flow chart depicting alternate aggressor path and the detection opportunities along those paths. Tabulated data is then used to evaluate the detection probability considering all of the possible mitigating circumstances. CTI is currently automating this process, utilizing hypertext links to facilitate information interconnections. Additionally, CTI is utilizing the CARVER methodology, which is a more qualitative, target selection process, with increased focus on airport overall risk assessment. Testing is used to validate the findings.

Lockwood Greene Technology

The Lockwood Greene Team is performing a quantitative analysis using a technique known as AVAT (Advanced Vulnerability Assessment Technique). AVAT is a derivative of the ASSESS model developed for use by the DOE, and utilizes portions of the ASSESS databases. The implementation is more of a spreadsheet style form, organized by layers, with detection, assessment, delay and response values. Further, an Adversary Intercept Diagram is developed to analyze response force actions. Testing is used to validate inputs to the assessment technique.

Naval Facilities Engineering Service Center (NFESC)

DOD experience is applied to the airport assessment project by the Risk Analysis Vulnerability Assessment (RAVA) Team from the NFESC. The RAVA methodology is largely a manual process, using expert judgement and structured questionnaires to quantify the airport vulnerability and risks. Supplemental information is provided by utilizing automated tools for explosive blast effects, and the Security Assessment Model (SAM). The RAVA Team makes extensive use of testing to verify the perceived vulnerabilities. These tests are highly structured, well coordinated, video recorded and are non-disruptive to airport operations or passengers.

Science Applications International Corporation (SAIC)

SAIC uses a "table top" approach which is very simple and straightforward. The Team conducts a normal data gathering phase, and then performs an interactive analysis involving airport security and law enforcement personnel. During this interactive table top session, agreement is reached on qualitative judgements of the security system detection, assessment and response capability. Numbers are applied to these "expert opinions" and calculations of vulnerability and relative risk are provided by an MS Excel spreadsheet. Countermeasure sets are then assessed as to their effect on risk, and costs to implement are estimated. SAIC does not include testing in their process.

Science & Engineering Associates (SEA)

The SEA team uses a highly quantitative approach involving the use of the tool, Analytical Software System for Evaluation of Security Safeguards (ASSESS). Sandia

National Laboratory, Livermore National Laboratory and SEA originally developed this tool for the assessment of DOE. SEA has begun modification of the code toward an airport oriented version of ASSESS, utilizing portions of the underlying database of security component detection and delay data. SEA depends upon testing to verify timing information and unique detection situations. The SEA Team conducts tests to verify vulnerabilities determined by preliminary analysis. The testing process is highly structured and non-intrusive.

Blue Ribbon Panel

The intent of the project was to conduct airport vulnerability assessments, and as a by-product to examine the processes used by various contractors and to determine the "best practices". To advise the FAA and to assist in the evaluation process, a Blue Ribbon Panel (BRP) was established with security professionals not involved in the assessments. The panel has members from the US Army Corps of Engineers and the National Laboratories (Argonne, Brookhaven, Oak Ridge and Sandia). A highly structured evaluation process is being applied to the evaluation of the contractors' plans and analysis reports. Also, feedback is obtained from the airport recipients of the reports and the FAA agents involved in the assessments. The feedback indicates, from the end-user's point of view, the value, quality and usefulness of the contractor's products and processes. The BRP is tasked to recommend a method to proceed with for future FAA sponsored airport vulnerability assessments. Further, the BRP is tasked to examine the available automated tools demonstrated in these assessments, and to recommend to the FAA a roadmap for proceeding to a tool (or set of tools) which are suitable to use in the field.

Airport Assessment Results

As would be expected, the results of the widely varied methodologies, applied to a set of diverse airports, are anything but identical. It is not the purpose of this paper to divulge specific findings for named airports. However, there are interesting trends and inconsistencies which are noteworthy and these can be discussed with airport anonymity.

Compliance

One of the general findings which is uniform is that the airports studied are predominantly in compliance with the FAA regulatory requirements. The Threat Scenarios prepared for this analysis were known to probe into area which are not highly regulated, but which are plausible terrorist approaches. Therefore, some of the scenarios result in relatively high calculated levels of vulnerability, and, for the most part, the highest vulnerabilities are logically predictable.

SIDA

Airports utilize a personnel identification security feature known as the Security Identification Display Area (SIDA). Each airport defines the SIDA in their Airport Security Plan, and it includes the security sensitive areas of the airport operations, such as the ramp area immediately surrounding parked aircraft. In this area, all personnel are required to display their ID badge (above the waist on their outermost garment). Furthermore, all employees are trained in SIDA practices, and are required to challenge any person in the SIDA area without a displayed badge.

The degree to which the SIDA practices are adhered to and enforced varies drastically among airports. Some approach the issue by providing incentives, such as small cash awards, for properly challenging a test subject. Many airports have the authority to issue "tickets" to anyone found not to challenge an unbadged person. Some of the punitive methods are so harsh that they are rarely enforced, which renders them useless. The best examples appear to be sites that combine active incentive programs with moderate (but enforces) punishments. But the dominant characteristic that is present at airports with good SIDA challenge practices is a high level of employee security awareness, the source of which is elusive.

Screening Point Staffing

Even prior to this study, it was a well-established fact that the screeners who man the airport checkpoints are subject to very high turnover rates. This can be explained in large part to the very low wage scale (minimum wage), the stress associated with the security responsibility of the screener, and the lack of job satisfaction (boredom, abuse by the public). There are many emerging technologies that will directly effect the screeners. New and more complex detection equipment may require a higher or different level of screener perception and training. Threat image projection systems should increase screener vigilance, improve detection of more types of threat objects, and provide a means of measuring screener proficiency. Screening point equipment improvements can only be effective if used by capable screeners.

Perimeter

Most airports have perimeter fences or natural barriers which are intended to impede an intruder from entry into the Air Operations Area (AOA). Analyses of threat scenarios that involve perimeter incursions indicate that the perimeter barriers provide only a small degree of delay to the intruder. Once inside the AOA, an intruder may have unimpeded access to aircraft or secured portions of the airport facilities, with varying degrees of potential detection by roving police patrols and/or employees who may of may not challenge intruders. Those airports that have installed Perimeter Intrusion Detection Systems and have adequate lighting and CCTV surveillance capabilities are much less vulnerable in these scenarios.

Access Control

Most airports have access control systems that control doors and/or gates from the public side of the airport to the secure side. Frequently, the personnel ID card is also used as the access control media. In some airports, the access control system has characteristics that greatly improve the security posture. For guarded gate control, the access control system can provide to the guard, a picture of the badge-holder for identity verification. For controlled doors, upon alarm the system can immediately display the camera image associated with that door (and is some cases, a "history" of that camera signal at or just before the alarm time) to the person responsible for assessing the alarms and initiating law enforcement dispatch.

Law Enforcement Staffing

Generally, the law enforcement practices observed at the airports were very professional with well-documented procedures. The ability to respond to threatening events at the screening points in a timely manner was generally adequate. One consistent shortfall however is the ability for timely response to other airport locations and the frequency of roving patrols. This is a direct result of the level of staffing that is established for the airport.

Countermeasures

The range of potential countermeasures identified by the contractors is as wide and varied as the approaches being used. However, the following list is representative of frequently mentioned security improvements. In many cases the airport specific cost-benefit analysis will dictate the appropriateness of the specific countermeasure.

Security awareness and training

- Screener training
- SIDA Challenge awareness for all badged employees

Policy and Procedures

- Background checks (more extensive, periodic updates)
- Positive Passenger Baggage Matching
- Employee screening
- Pre-flight aircraft inspections
- Random screening – checked baggage, cargo

Equipment

- Upgrade screening point equipment
- Perimeter intrusion detection systems
- Improved lighting and surveillance
- Enhanced CCTV (digital recording, exterior coverage, alarm linkage)

Lessons Learned

The foremost lesson learned from the execution of this project is the effectiveness of detailed, comprehensive and timely coordination. The potential exists for significant disruption of airport and air carrier personnel activities in the process of gathering the information necessary to carry out the extensive analysis to be performed. However, through the advanced acquisition of key documentation, introductory coordination briefings, and the designation of an FAA lead at each site for coordination, this project has achieved a minimal level of disruption.

Testing activities have also generated several lessons. Coordination of test plans with all effected parties is essential. In some cases, it is also essential to keep the test subjects unaware of the test to keep the results unbiased. Coordination with managers of the staff under test must be accompanied with explicit instructions to keep the test blind. The response of an organization to testing situations must be carefully observed, and unusual staffing arrangements at the time of planned testing is likely to indicate an intent to skew the test results.

Safety is the most important aspect of test planning. In airport testing, no live explosives or functional weapons are ever used. High fidelity explosive simulants have been developed specifically for airport site testing. Dummy detonators and disabled weapons are used and serve the purpose of detectability by the screening equipment without being a safety hazard. Controllers are used extensively to step in at any point of potential conflict between the mock adversary and an airport employee or security person.

Where to from Here?

By the end of this fiscal year, all 15 airport assessment will be completed. The Blue Ribbon Panel will determine the quality/effectiveness of each of the approaches and by December 1998 will have a recommendation to the FAA. The funds appropriated for continued Airport Vulnerability Assessment in FY99 will then be used to proceed with additional assessment performed by the selected contractor(s).

By March 1999, the Blue Ribbon Panel will provide to the FAA a recommendation on how to proceed with automated tools for field use. If one of the existing tools is deemed appropriate, then the FAA could proceed with immediate implementation. If product improvement is called for, the FAA must determine the best manner for bringing the products up to the required capabilities. Ultimately, the FAA plans to have a standardized practice, augmented by automated tools, for assessing airport vulnerability at a local level.